REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 14-16 stand rejected under 35 USC 112, second paragraph, as being indefinite. The claims are amended to obviate this rejection.

Claim 1-3, 5-11 and 13-23 stand rejected under 35 USC 102 as allegedly being anticipated by Stewart. In response, claims 1, 6, and 17 are amended here with to obviate the rejection. Claim 13 is amended to include the limitations of claim 14 therein, and as such the rejection is traversed.

Stewart teaches a system where a number of different users can receive access to the Internet, and can receive different levels of access. According to one embodiment described by Stewart, user identification is used to determine which of the different levels of access are provided. A number of different embodiments are also disclosed by Stewart. The embodiment bridging columns 9-10 discloses use of multiple different quality of service metrics. There are a number of different access points on the system. The embodiment at the bottom of column 10 allows selecting which of a plurality of different access points to use. The system ID is used to carry out the selecting. column 11 lines 17-33 suggest that the different system IDs may

prove correspond to different network providers. Column 13 describes that the privilege level indicates which network resources the user may access, and that one of these privilege levels only allow certain access to resources

The present application, however, discloses, and now claims, a very different kind of system. An important feature, now defined by claim 1, recites that there are different and separate communication parts and that the access to these parts is controlled by different secret keys. This substantially simplifies the system, and makes it easier to obtain access. More specifically, claim 1 defines a first communication part defining a first class of service that includes access to files and a second communication part that transmits a separate communication stream over substantially the same area and defines a second class of service. The first communication part is accessed by using a secret key and automatically provides access to users that have the secret key. The second communication part allows access without the secret key.

In this way, communications and the amount of access is easily controlled: simply by determining whether the user has, or does not have, the secret key. Stewart is much more complicated, since it requires that the user credentials be checked and verified. While Stewart does allow access based on SSID, it does not disclose the now claimed subject matter of automatically

allowing access based on possessing a secret key. SSIDs are not secret keys, as claimed.

Claim one also defines sets of permissions, where one of the sets of permission comprises access to files, where the user is granted access to the files when they have the encryption key but not granted access to the files when they do not have the encryption key. The rejection states that Stewart's column 14 and 16 disclose this subject matter. However, the cited section of column 14 merely discloses private portions on the network. The cited section of column 16 again describes that different computing resources can be stored on the network. It does not disclose that users with an encryption key can access files on the network, but users who do not have the encryption key cannot access those files as defined by claim 1. Therefore, claim 1 is not anticipated by Stewart.

Claim to defines a greater speed of network access, and with all due respect, this is nowhere disclosed or suggested by Stewart.

Claim 4 similarly defines limited upload and download speed. In rejecting claims 2 and 4, the rejection states that it would be obvious to do this, based on the disclosure in Stewart that states that it is desirable to limit the amount of bandwidth. While this may be true, there is nothing in Stewart that discloses or in any way suggests that the different levels of access have different access to bandwidth. The only thing

Stewart says about bandwidth appears to be in column 19 lines 5-8 and 45-48. Stewart discloses that it is good to limit the bandwidth so that more subscribers can be accommodated. There is no disclosure the different subscribers receive different levels of bandwidth access; more specifically, greater speed of network access as in claim 2 or more limited upload and download speeds for Internet as in claim 4.

Claim 3 defines a third communication part, defining a third class of service with third sets of permissions. This third set of permissions allows access to only specified Internet site. Therefore, collectively, claim 3 allows three different sets of permissions: the highest level of permission, the second level of permission which does not provide access to files, and the third level of permission which provides access to only specified Internet sites. Nothing in Stewart suggests such a three layer of access.

Claim 5 defines even further patentable details, where the first and second levels are based on secret keys, and the third level is granted when no key is available. This further simplifies the access granting mechanism.

Claim 6 has been amended to recite that access is automatically granted to users having the first secret key, and that the second wireless network portion can be accessed by users not having the second secret key. This claim should be allowable along with the claims which depend therefrom.

Claim 7 specifies an amount of bandwidth.

Claim 9 defines that there are separate wireless network interface cards operating in the same location forming the different networks. This is not disclosed by Stewart.

Claim 10 defines the third layer of network access further undisclosed by the cited prior art. Claim 11 defines that the key is an encryption key, which is not disclosed or suggested by the cited prior art.

In rejecting claim 12, the rejection takes official notice that a digital certificate can include an encryption key. The rejection further states that column 12 lines 4-15 explain that Stewart may use a digital certificate. However, this digital certificate is used as "other ID", see column 12 line 8. There is no disclosure of automatically granting access based on possession of an encryption key, as defined.

Claim 13 has been amended to include the limitations of claim 14 therein. As described above, there is no teaching or suggestion of different levels of access based on different possessions of encryption keys.

Claim 17 further defines similar subject matter to that discussed above with respect to claim and should hence be allowable for similar reasons to those discussed above, specifically that it defines the three different levels of service.

Claim 21 defines the automatic granting, the advantages of which have been disclosed in detail above.

Note that these advantages are not disclosed or contemplated by the prior art, and certainly not obvious based thereon. Nothing in the prior art suggests the advantage of automatically granting access based on the possession of a secret key as in claim 1 and others. Nothing in the prior art teaches multiple different networks, each having a different capability, and one of which can be accessed depending on which of the keys is obtained as in claim 3 and others. Different ones of the claims define different aspects of the above, and the advantages of this are not recognized by the prior art. Therefore, these claims should be allowable for these reasons.

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

For all of these reasons, it is respectfully suggested that all of the claims should be in condition for allowance. A formal notice of allowance is hence respectfully requested.

If the Examiner believes that communications such as a telephone interview or email would facilitate disposal of this case, the undersigned respectfully encourages the Examiner to contact the undersigned.

Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail (using the email address scott@harrises.com). I understand that a copy of these communications will be made of record in the application file.

Please charge any fees due in connection with this response to Deposit Account No. 50-1387, small entity.

Respectfully submitted,

Date: _12/18/07_____

__/Scott C Harris/_____
Scott C. Harris
Reg. No. 32,030

Customer No. 23844
Scott C. Harris, Esq.
P.O. Box 927649
San Diego, CA 92192
Telephone: (619) 823-7778
Facsimile: (858) 756-7717